INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	10627281
Filing Date	2003-07-25
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2132
Examiner Name	HO, Thomas M
Attorney Docket Number	MS1-1275US

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5272755		1993-12-21	Miyaji, ; et al.	
	2	6968354		2005-11-22	Kaminaga, ; et al.	
	3	6986054		2006-01-10	Kaminaga, ; et al.	
	4	7079650		2006-07-18	Knudsen	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030072443	A1	2003-04-17	Harley, Robert Joseph; et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /GB/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	10627281
Filing Date	2003-07-25
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2132
Examiner Name	HO, Thomas M
Attorney Docket Number	MS1-1275US

	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	BARRETO, PAULO S.L.M., et al., "Efficient Algorithms for Pairing-Based Cryptosystems," Universidade de Sao Paulo, Escola Politecnica, Sao Paulo (SP), Brazil & Computer Science Department, Stanford University, USA, pp. 1-16.	☐
	2	Boneh, et al., "Identity-Based Encryption from the Weil Pairing," SIAM J. COMPUT., Vol 32, No. 3, pp. 586-615, 2003 Society for Industrial and Applied Mathematics.	☐
	3	Boneh et al., "Short signatures from the Weil pairing," pp. 1-17.	☐
	4	Cantor, "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, Vol. 48, No. 177, January 1987, pp. 95-101.	☐
	5	Eisentrager, et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," Topics in Cryptology, CT-RSA 2003, Marc Joye (Ed), pp. 343-354, LNCS 2612, Springer-Verlag, 2003.	☐
	6	FREY, GERHARD et al., "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, April 1994, pp. 865-874.	☐
	7	Frey, et al., "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems", IEEE Transactions on Information Theory, Vol. 45, NO.5, July 1999, pp 1717-1719	☐
	8	Galbraith, et al., "Implementing the Tate Pairing," Mathematics Dept., Royal Holloway, University of London, Egham, Surrey, UK & Hewlett-Packard Laboratories, Bristol, Filton Road, Stoke Gifford, Bristol, UK, pp. 1-14.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /GB/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	10627281
Filing Date	2003-07-25
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2132
Examiner Name	HO, Thomas M
Attorney Docket Number	MS1-1275US

	9	HESS, FLORIAN et al., "Two Topics in Hyperelliptic Cryptography," S. Vaudenay & A. Youssef (Eds.): SAC 2001, LNCS 2259, 2001, pp. 181-189.	☐
	10	JOUX, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey),"C. Fieker and D.R. Kohel (eds.): ANTS 2002, LNCS 2369, pp. 20-32, 2002 (Springer-Verlag Berlin Heidelberg 2002).	☐
	11	Koblitz, "Elliptic Curve Cryptography", 01/05/2007, at <<http://www.msri.org/publications/ln/msri/1998/crypt/koblitz/1/banner/01.html>>, MSRI, January 11, 1998, pp 1-34	☐
	12	MENEZES, ALFRED J., et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," (0018-9448/93 1993 IEEE, IEEE Transactions on Information....), 8 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Gilberto Barron Jr/	Date Considered	05/13/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /GB/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	10627281
Filing Date	2003-07-25
First Named Inventor	Anne Kirsten Eisentraeger
Art Unit	2132
Examiner Name	HO, Thomas M
Attorney Docket Number	MS1-1275US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Chris Culberson/	Date (YYYY-MM-DD)	2007-05-18
Name/Print	Chris Culberson	Registration Number	59136

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /GB/